Standards Overview for the DoD PKI Technical Working Group

John Samanick / Greg Scott
JIEO Center for Information Technology Standards
samanicj@ftm.disa.mil / scottg@ftm.disa.mil
May 2000

Web Pages

For additional details and to obtain copies of products discussed

- **For PKI:**

  http://www-pki.itsi.disa.mil/

- **For Directory:**

  http://www-ds.itsi.disa.mil/

Network Applications and Security Branch - PKI Work

JEBBB - Ed Richards

PKI

- John Samanick
- Greg Scott

DIRECTORY

- Bill Curtin
- Kristin McAuliffe
- Maureen Kirlin

DMS

- Nelson Alvarez
- Vince Chin

PKI and Directory Tactical Extension

- Bill Scott

LAN Management

- Maureen Kirlin (part time)

PKI Standards Support

- **CFITS role:**
  - **Investigate PKI features and protocols for DoD requirements versus commercial standards, identify difference, and work to align standards with requirements**
  - **Recommend Standards for inclusion in the JTA**
- **Prioritization of feature/protocol analyses established with PKI Chief Engineer**
  - **Program's fast pace makes priorities very fluid**
- **Focus is on interface between multi vendor secure COTS applications and the DoD PKI**
  - **Interoperability with external (non-DoD) PKI is needed but a secondary effort**

Standards Sources

ITU/ISO - X.509, other X.5xx series

IETF - X.509 profile, OCSP, LDAP, IPsec, other applications, etc.

ANSI - X9 series algorithms

RSA - PKCS series

PKI Forum - Demos, testing, results/lessons learned, recommendations

NIST - Algorithm FIPS

Federal PKI TWG - policy, X.509 profile, CONOPS, and MISPC

DoD - JTA, requirements, specifications, procedures

NSA - SDN series, security profile, policy

PKI Interface Protocols

- SCEP - Simple Certificate Enrollment Protocol
- CMS - Cryptographic Message Syntax
- CMC - Certificate Management Messages over CMS
- HTTP - HyperText Transfer Protocol
- FTP - File Transfer Protocol
- LDAP - Lightweight Directory Access Protocol
- CMP - Certificate Management Protocol
- SCVP - Simple Certificate Verification Protocol
- TSP - Time Stamp Protocol
- DCVS - Data Validation and Certification Server Protocol
- OCSP - Online Certificate Status Protocol
- CRMF - Certificate Request Message Format
- TLS - Transport Layer Security

PKI Relationships

SECURE APPLICATIONS

IPsec S/MIMEv3 Legacy Application TLS

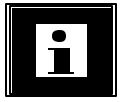
STIME DNSsec PKI Middleware SecSH

INTERFACE PROTOCOLS

SCEP CMS CMC HTTP FTP LDAP
CMP SCVP TSP DCVS OCSP CRMF
TLS

PUBLIC KEY INFRASTRUCTURE

CA RA/LRA KE OCS WEB FTP TSA DS



http://www...

ftp://ftp...

***Functions contained in DOD PKIv2 in shaded areas**

Standards cited in the JTA

- **Mandated Standards**
  - **ITU-T X.509v3, June 1997**
  - **FIPS 140-1, 180-1**
- **Emerging Standards**
  - **RFCs 2314, 2315, 2459, 2559, 2587**
  - **FIPS 46-3 (Draft)**
  - **Federal PKI X.509 Certificate and CRL Extensions Profile, 9 March 1998**
  - **RSA PKCS #1, 11, 12**
  - **DoD Medium Assurance PKI Functional Specification (Draft), 20 October 1998**

Branch Major PKI Products 2000

- Mapping of DOD requirements to standards
- Object signing analysis
- OCSP DOD Profile
- Installation of DOD PKI version 2, S/MIMEv3, and IPsec routers in CFITS Analysis Facility
- Analysis of CRMF standard against DOD PKI & Microsoft 2000
- S/MIMEv3 with DOD PKIv2 analysis
- IPsec related profile(s)

Mapping of DOD requirements to standards

- **Purpose: Identify work areas in standards.**
- **Source: DoD Target PKI User Requirements, 29 Feb 00**
- **Process: Filter requirements to be met by system engineering or policy.**
- **Remaining standards requirements are mapped against current IETF standards.**
- **Identify areas of standards work - a requirement is not met, prepare draft standard, check out in our facility, and then propose to the IETF.**

Object signing analysis

- **Purpose: Determine if it is useful to deploy object signing certificates based on current standards**
- **RFC 2459 defined a code signing key purpose for the Extended Key Usage (EKU) extension.**
  - **Not used in current commercial software publisher certificates**
  - **What is the CA actually certifying about a signer?**
    - **The signer's identity**
    - **Perhaps a pledge to protect against malicious code**
  - **What can the RP trust about the certified signer?**
    - **The signer's identity.**
    - **There is no tie in to policy or commercial best practices. No clear liability chain in the case of malicious code.**
- **Do not recommend its use.**

Object signing analysis (continued)

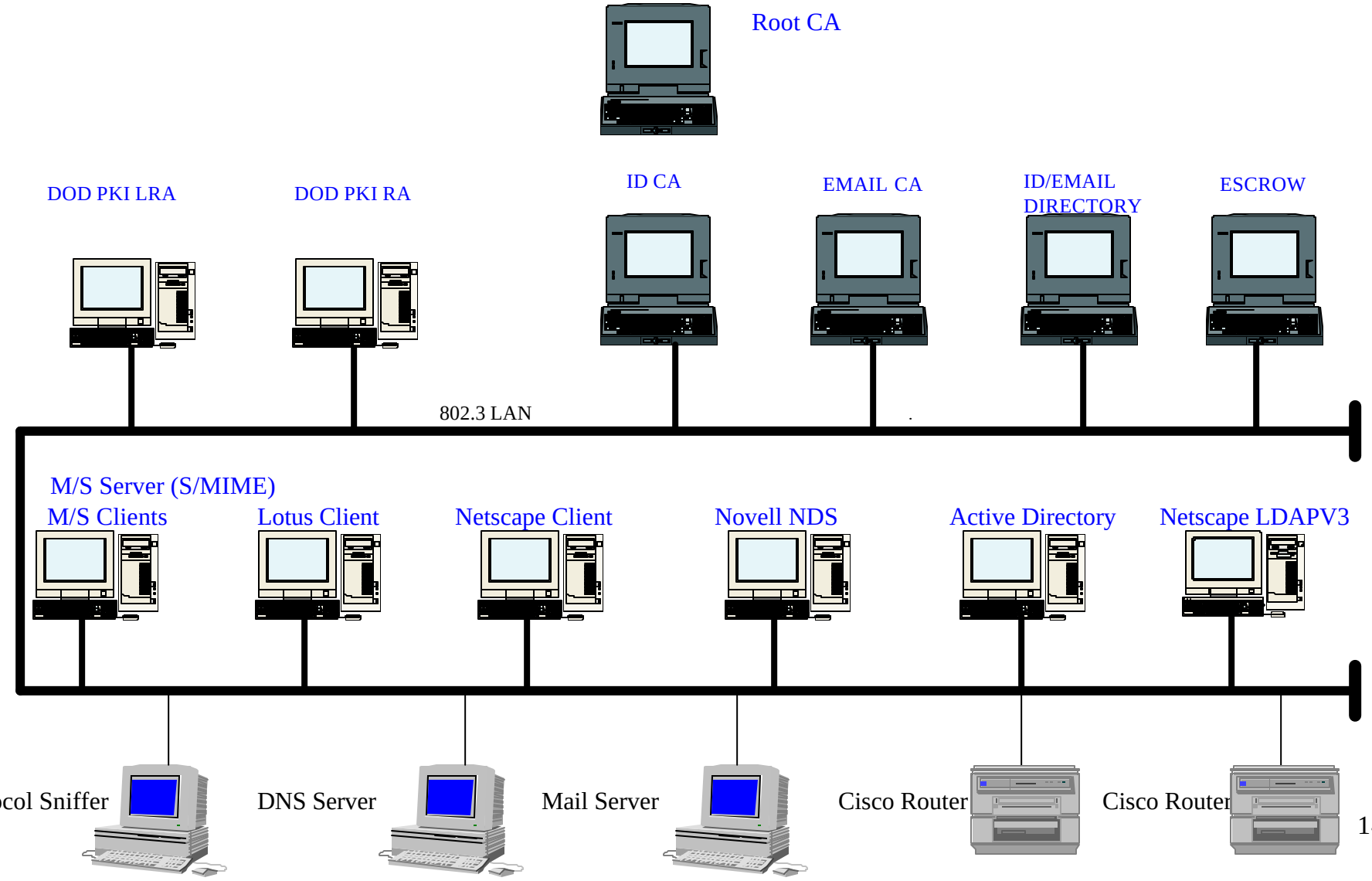
- X.509v4 defines an attribute certificate
  - Binds a privilege to identity.
  - Contains no public key
  - The Attribute Authority (AA) is trusting the privilege holder to adhere to policy that is not enforceable by technical means.
    - Who bears liability?
  - Steps before implementation:
    - Is there an actual requirement? Does this meet it?
    - Vendor implementations?
    - Who is the AA?
    - Privilege policies?

OCSP DOD Profile

- **Purpose: Profile RFC 2560, Online Certificate Status Protocol (OCSP) for the benefit of vendors and DOD users.**
- **Draft profile will be made available at:**

  http://www-pki.itsi.disa.mil/pkiprofiles.htm
- **Analysis DOD PKIv2 OCSP Profile facility**

STANDARDS ANALYSIS NETWORK
DoD PKI V2.0, DIRECTORY, S/MIME



STATUS OF MAJOR S/W PACKAGES

- **DoD PKI V2.0: Installing replica of the fielded software on Facility Sun Workstations.**
  - **Status: Packages loaded on each machine. Configuration still ongoing.**
- **LDAP DIRECTORY PRODUCTS: Novell eDirectory, Microsoft Active Directory, and Netscape Directory v4.1 loaded on Facility PCs.**
  - **Status: Packages loaded and configured. Evaluations ongoing.**
- **S/MIME V3 PRODUCTS: Microsoft Outlook 2000 SR1, Others TBD**
  - **Status: M/S with S/MIMEv3 loaded and configured. Evaluation ongoing.**

Certificate Request Message Format (CRMF)

- **Purpose: Evaluate CRMF differences between standards and major vendor PKI products.**
- **Latest Netscape (via DoD PKI) and Microsoft 2000 products to be evaluated to determine current state of interoperability for certificate requests**

S/MIMEv3 Analysis

- **Purpose: Evaluate S/MIMEv3 capabilities with DoD PKI requirements and capabilities**
- **Evaluate S/MIMEv3 against the DoD PKI V2.0**
- **Evaluate standards including Messaging, Certificate Handling, Cryptographic Message Syntax, and Certificate Distribution Spec**
- **S/MIMEv3 compliment to STANAG 4406**

IPsec-Related Profiles

- **Purpose: Map DoD IP security requirements to Simple Certificate Enrollment Protocol (SCEP) developed by Cisco.**
- **Evaluate "person in the middle" capability of SCEP required by DoD policy**
- **Identify industry convergence to SCEP (or other protocols)**
- **Evaluate protocol using Cisco routers and Netscape CEP**
- **Develop profile(s) based on evaluation results**

GIG Directory Standards Support

- **CFITS role:**
  - **Investigate Directory features and protocols for DOD requirements versus commercial standards, identify difference, and work to align standards with requirements**
- **Prioritization of feature/protocol analyses established with Directory Chief Engineer**
  - **Program's fast pace makes priorities very fluid**
- **Focus is on multi vendor COTS Directory interoperability**
  - **Recognition that interface with multi vendor applications is needed but secondary effort**

Branch Major GIG Directory Products CY2000

- DOD requirements mapped to core LDAPv3 stds
- COTS basic LDAP Replication analysis
- Determine LDAP Replication elements of service
- DOD requirements mapped to related RFCs
- DOD requirements mapped to Internet Drafts
- Vendor conformance to replication standards
- Analyze and acquire meta-directory COTS products
- Map COTS LDAP products to requirements & standards
- Map COTS meta-directory products to requirements & stds

Tactical Extensions Standards Support

- **Purpose: Identify candidate commercial protocol standards that may benefit tactical (or deployed) fielding of PKI technology. Determine availability of these protocols in COTS products.**
- **Standards Analysis Facility PCs configured with tactical lower layer protocol (e.g. MIL-STD-188-184) running commercial browser applications.**
- **Run applications interacting with DoD PKI to determine capabilities and problem areas.**
- **Make recommendations on applicable COTS protocols for insertion into the Joint Technical Architecture.**

Protocols of interest include

- OCSP
- LDAP Control Extension for Simple Paged Results
- Low Infrastructure Public Key Mechanism using SPKM
- Certificate-based Roaming
- Wireless Transport Layer Security Protocol (WTLS)
- WTLS MiniCerts.